**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

Serial No. .....
Filing Date .....
Inventorship ..... Venkatesan et al
Applicant ..... Microsoft Corporation
Attorney's Docket No. ..... MS1-1922US
Title: Primitives for Fast Secure Hash Functions and Stream Ciphers

## INFORMATION DISCLOSURE STATEMENT

*References* -- See Attached Form PTO-1449

## REMARKS

The citations listed, copies attached, are submitted in compliance with the duty of disclosure defined in 37 CFR §1.56. The Examiner is requested to make these citations of official record in this application.

Respectfully Submitted,

Date: 2/9/04

By: Ramin Aghevli
Ramin Aghevli
Reg. No. 43,462

Please type a plus sign (+) inside this box → [+]

EV 395542223

Substitute for form 1449A/PTO

# INFORMATION DISCLOSURE STATEMENT BY APPLICANT

*(use as many sheets as necessary)*

Sheet 1 of 3

| Complete if Known | |
|---|---|
| Application Number | |
| Filing Date | |
| First Named Inventor | Venkatesan |
| Group Art Unit | |
| Examiner Name | |
| Attorney Docket Number | MS1-1922US |

## U.S. PATENT DOCUMENTS

| Examiner Initials* | Cite No.[1] | U.S. Patent Document Number | Kind Code[2] (if known) | Name of Patentee or Applicant of Cited Document | Date of Publication of Cited Document MM-DD-YYYY | Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear |
|---|---|---|---|---|---|---|
| | | 6,496,928 | | Deo et al | 12-17-2002 | |
| | | 6,275,599 | | Adler et al | 08-14-2001 | |
| | | 5,673,316 | | Auerback et al | 09-30-1997 | |
| | | 5,651,069 | | Rogaway | 07-22-1997 | |
| | | 3,962,539 | | Ehrsam et al. | 06-08-1976 | |
| | | 4,200,770 | | Hellman et al | 04-29-1980 | |
| | | 4,218,582 | | Hellman et al. | 08-19-1980 | |
| | | 4,309,569 | | Merkle | 06-05-1982 | |
| | | 4,405,829 | | Rivest et al. | 08-20-1983 | |
| | | 4,625,076 | | Okamoto et al. | 11-25-1986 | |
| | | 4,748,668 | | Shamir et al. | 05-31-1988 | |
| | | 4,850,017 | | Matyas, Jr. et al | 07-18-1989 | |
| | | 4,850,019 | | Shimizu et al. | 07-18-1989 | |
| | | 4,908,861 | | Brachtl et al | 03-13-1990 | |
| | | 4,995,082 | | Schnorr | 02-19-1991 | |
| | | 5,140,634 | | Guillou et al | 08-18-1992 | |
| | | 5,214,703 | | Massey et al | 05-25-1993 | |
| | | 5,231,668 | | Kravitz | 07-27-1993 | |
| | | 5,276,737 | | Micali | 01-04-1994 | |
| | | 3,798,359 | | Feistel | 03-19-1974 | |

## FOREIGN PATENT DOCUMENTS

| Examiner Initials* | Cite No.[1] | Foreign Patent Document Office[3] | Number[4] | Kind Code[5] (if known) | Name of Patentee or Applicant of Cited Document | Date of Publication of Cited Document MM-DD-YYYY | Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear | T[6] |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

| Examiner Signature | | Date Considered | |
|---|---|---|---|

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Unique citation designation number. [2] See attached Kinds of U.S. Patent Documents. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

Please type a plus sign (+) inside this box → [+]

EV395542223

Substitute for form 1449A/PTO

# INFORMATION DISCLOSURE STATEMENT BY APPLICANT

*(use as many sheets as necessary)*

Sheet 2 of 3

| *Complete if Known* | |
|---|---|
| Application Number | |
| Filing Date | |
| First Named Inventor | Venkatesan |
| Group Art Unit | |
| Examiner Name | |
| Attorney Docket Number | MS1-1922US |

## U.S. PATENT DOCUMENTS

| Examiner Initials* | Cite No.[1] | U.S. Patent Document Number | Kind Code[2] (if known) | Name of Patentee or Applicant of Cited Document | Date of Publication of Cited Document MM-DD-YYYY | Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear |
|---|---|---|---|---|---|---|
| | | 4,386,233 | | Smid et al. | 05-31-1983 | |
| | | 4,424,414 | | Hellman et al. | 01-03-1984 | |
| | | 4,567,600 | | Massy et al | 01-28-1986 | |
| | | 4,633,036 | | Hellman et al. | 12-30-1986 | |
| | | 4,881,264 | | Merkle | 11-14-1989 | |
| | | 4,956,863 | | Goss | 09-11-1990 | |
| | | 5,003,597 | | Merkle | 03-26-1991 | |
| | | 5,016,274 | | Micali et al. | 05-14-1991 | |
| | | 5,299,262 | | Brickell et al | 03-29-1994 | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

## FOREIGN PATENT DOCUMENTS

| Examiner Initials* | Cite No.[1] | Foreign Patent Document Office[3] | Number[4] | Kind Code[5] (if known) | Name of Patentee or Applicant of Cited Document | Date of Publication of Cited Document MM-DD-YYYY | Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear | T[6] |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

| Examiner Signature | | Date Considered | |
|---|---|---|---|

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Unique citation designation number. [2] See attached Kinds of U.S. Patent Documents. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

Please type a plus sign (+) inside this box → [+]

EV 395542223

Substitute for form 1449B/PTO

# INFORMATION DISCLOSURE STATEMENT BY APPLICANT

*(use as many sheets as necessary)*

Sheet 3 of 3

| *Complete if Known* | |
|---|---|
| Application Number | |
| Filing Date | |
| First Named Inventor | Venkatesan |
| Group Art Unit | |
| Examiner Name | |
| Attorney Docket Number | MS1-1922US |

## NON PATENT LITERATURE DOCUMENTS

| Examiner Initials* | Cite No.[1] | Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published. | T[2] |
|---|---|---|---|
| | | MENEZES, A., van OORSCHOT, P., and VANSTONE, S.; Chapter 9, "Hash Functions and Data Integrity" from Handbook of Applied Cryptography CRC Press 1996 pgs 321 to 383 | |
| | | MENEZES, A., van OORSCHOT, P., and VANSTONE, S.; Chapter 6, "Stream Ciphers" from Handbook of Applied Cryptography CRC Press 1996 pgs 321 to 383 | |
| | | BENJAMINI, I., BERGER, N., HOFFMAN, C., MOSSEL, E.; "Mixing Times of the Biased Card Shuffling and the Asymmetric Exclusion Process" Submitted for Publication October 9, 2002 22 pages | |
| | | MIRONOV, ILYA; "(Not So) Random Shuffles of RC4" Advancesin Crytology, CRYPTO 2002, 19 pages | |
| | | MANTIN, ITSIK; "RC4 Webpage" http://www.wisdom.weizmann.ac.il/~itsik/RC4/rc4.html 2 pages | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

| Examiner Signature | | Date Considered | |
|---|---|---|---|

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Unique citation designation number. [2] Applicant is to place a check mark here if English language Translation is attached.